HPSR Software Security Content

2014 Update 3

September 30, 2014

HP Software Security Research is pleased to announce the immediate availability of updates to HP Application Defender, HP WebInspect SecureBase (available via SmartUpdate), the HP Fortify Secure Coding Rulepacks (English language, version 2014.3.0), and HP Fortify Premium Content.

About SSR

The Software Security Research team translates cutting-edge security research into security intelligence that powers the HP Enterprise Security Products portfolio. Today, HPSR Software Security Content supports over 880 vulnerability categories across 22 programming languages and spans more than 806,000 individual APIs.

HP Application Defender

Managed from the cloud, HP Application Defender is a software-as-a-service (SaaS) solution that protects production applications against software security vulnerabilities. For the inaugural release, the Software Security Research team provides **15** distinct vulnerability categories, including the following feature highlights:

GNU Bourne Again Shell (bash) 'Shellshock' rulepack

- A rulepack update is available for immediate use to protect applications deployed on common Java application servers against the highly publicized 'Shellshock' vulnerability as mentioned in CVE-2014-6271 and CVE-2014-7169.

Known scanner activity detection

- The ability to detect and act upon reconnaissance activity generated from automated scanners is an essential capability to disrupt the adversary early in the attack lifecycle.

Malformed request detection

- Simply removing headers from an HTTP request can wreak havoc upon your production applications. Similarly, referencing HTTP methods that aren't explicitly supported by your application may cause unexpected behavior. HP Application Defender has you covered.

Solid baseline protection

- Protection against classic input injection attacks such as cross-site scripting, SQL injection, header manipulation, and XML external entity injection has been enhanced and incorporated into the core feature set, in addition to the following vulnerability categories:
  - Command injection
  - Directory listing
  - Forceful browsing
  - Poor error handling
  - Privacy violation [credit card and social security number]
  - System information leak

HP SecureBase (WebInspect)

SecureBase combines checks for thousands of vulnerabilities with policies that guide users in identifying critical weaknesses in web and mobile software.

Advisory support

In order to improve coverage of critical vulnerabilities, the following security content has been added to this quarterly update:

GNU Bourne Again Shell (bash) 'Shellshock' vulnerability

- A check is now available for immediate use to detect servers vulnerable to the highly publicized 'Shellshock' vulnerability as released in CVE-2014-6271.

OpenSSL ChangeCipherSpec injection

- An out-of-order processing of ChangeCipherSpec message in the OpenSSL library presents a critical threat to the message integrity and confidentiality assured by SSL/TLS. The update adds support for CVE-2014-0224.

HP Software Security Research
hp.com/go/ssr

Contact

Joe Sechman
Director, Software Security Research
HP Security Research
sechman@hp.com
+1 (770) 343 - 7052

Insecure Anonymous ECDH detection

- Support for detecting Denial of Service attacks caused by a NULL pointer dereference error in the OpenSSL library as described in CVE-2014-3470.

HP WebInspect Agent Technology

Struts ClassLoader Manipulation

- Support for server-agnostic detection of ClassLoader manipulation in Apache Struts as described in CVE-2014-0112 and CVE-2014-0114.

Email Injection

- Six new categories have been added to detect and describe vulnerabilities in an application when handling emails programmatically - SMTP/IMAP Header Injection, SMTP/IMAP/POP3 Command Injection, and Insecure email connections.

Compliance templates

OWASP mobile top ten risks 2014

- Support for the latest version of the 2014 top ten mobile risks released by the Open Web Application Security Project.

HP Fortify Secure Coding Rulepacks (SCA)

With this release the **Fortify Secure Coding Rulepacks** detect **618** unique categories of vulnerabilities across **22** programming languages and span over **806,000** individual APIs. In summary, the release includes the following:

Improved SAP ABAP support[1]

- A completely rewritten ABAP rulepack is now available to be used with the new SCA ABAP translator, which is provided as a Technology Preview[2]. This new rulepack provides improved accuracy of results and adds Cross-Client Data Access as a new vulnerability category.
- For all supported versions of SCA, the following new category is available: User or System Dependent Program Flow.

Ruby[1]

- New language support for Ruby 1.9 is provided as a Technology Preview[2].This new language support includes the Core and Standard libraries distributed with Ruby MRI, along with some of the commonly used third party libraries such as Rack, MySQL, and MySQL2.
- Support for 32 vulnerability categories is provided for Ruby, including the following new categories: Dynamic Code Evaluation: Unsafe Stream Deserialization, and Weak Cryptographic Hash: User Defined Salt.

GWT 2.x

- Support for Google Web Toolkit (GWT) 2.x including new protocols, widgets, and APIs introduced in latest versions.

Apple iOS and Google Android support

- Support for the Apple System Logging API as a source of System Information as well as coverage for both Privacy Violation and System Information Leak categories.
- Increased support for Android's CERT Coding Guidelines, covering typical problems within Android applications.

MX Injection / SMTP Header Injection

- Support for MX Injection and SMTP Header Injection categories across multiple libraries and frameworks including: Java's JavaMail, Spring Framework Mail, Spring Integration, Apache Commons Net, and Apache Commons Email; PHP's mail and imap libraries; and Python's smtplib, imaplib, and poplib libraries.
- New categories include: Mail Command Injection: IMAP, Mail Command Injection: POP3, Mail Command Injection: SMTP, Transport Layer Protection: Insecure Mail Transmission, and Header Manipulation: SMTP.

OWASP mobile top ten 2014

- Support for the latest version of the 2014 top ten mobile risks released by the Open Web Application Security Project.

[1] Requires HP Fortify SCA 6.20 for Technology Preview functionality.
[2] Technology Preview features are not yet supported, are not functionally complete, and are not suitable for deployment in production. These features are provided to the customer as a courtesy. The primary objective is to give planned features wider exposure, with the goal of providing full support in the future.

HP Software Security Research
hp.com/go/ssr

Contact

Joe Sechman
Director, Software Security Research
HP Security Research
sechman@hp.com
+1 (770) 343 - 7052

HP Fortify Premium Content

The research team builds, extends, and maintains a variety of resources outside our core security intelligence products.

OWASP mobile top ten report[3]

- A new report bundle with support for OWASP mobile top ten risks 2014 is available for download from the Fortify Customer Portal under Premium Content.

The Evolution of a Taxonomy: Ten Years of Software Security whitepaper

- This whitepaper describes how HP Security Research is extending the Seven Pernicious Kingdoms taxonomy into a common vocabulary used to describe software security vulnerabilities regardless of analysis technique.

Updated vulnerability knowledge bundles

- Both online and standalone versions of the vulnerability knowledge bundles have been updated to include categories covered by the extended taxonomy preview.

[3] Requires HP Fortify SSC 4.20.

Learn more at
hp.com/go/hpsr